

FortiOS™ Handbook - Compliance

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Wednesday, June 3, 2015

FortiOS™ Handbook - Compliance

01-520-129720-20141002

TABLE OF CONTENTS

Introduction	5
Before you begin	5
How this guide is organized	5
Configuring FortiGate units for PCI DSS compliance	6
Introduction to PCI DSS	6
What is PCI DSS?	6
What is the Cardholder Data Environment	6
PCI DSS objectives and requirements	6
Network topology	9
Internet	10
The CDE wired LAN	10
The CDE wireless LAN	11
Other internal networks	11
Security policies for the CDE network	11
Controlling the source and destination of traffic	11
Controlling the types of traffic in the CDE	12
The default deny policy	12
Wireless network security	12
On-wire detection of rogue APs	12
Setting up rogue access point scanning	12
Securing a CDE network wireless access point	13
Protecting stored cardholder data	14
Protecting communicated cardholder data	14
Configuring IPsec VPN security	14
Configuring SSL VPN security	15
Protecting the CDE network from viruses	15
Enabling FortiGate antivirus protection	15
Configuring antivirus updates	16
Enforcing firewall use on endpoint PCs	16
Monitoring the network for vulnerabilities	16
FortiGate logs	16
Using the FortiOS Network Vulnerability Scan feature	17
Monitoring with other Fortinet products	17
Restricting access to cardholder data	17

Controlling access to the CDE network 17

 Password complexity and change requirements.....17

 Password non-reuse requirement18

 Administrator lockout requirement19

 Administrator timeout requirement 19

 Administrator access security..... 19

 Remote access security..... 19

Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document discusses issues related to compliance, specifically Payment Card Industry Data Security Standard (PCI DSS).

This chapter contains the following topics:

- [Before you begin](#)
- [How this guide is organized](#)

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

[Configuring FortiGate units for PCI DSS compliance on page 6](#) explains the Payment Card Industry Data Security Standard (PCI DSS). It provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements.

Configuring FortiGate units for PCI DSS compliance

This chapter provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements. There is also some description of other Fortinet products that can help you with PCI DSS compliance. The following topics are included in this section:

- [Introduction to PCI DSS](#)
- [Network topology](#)
- [Security policies for the CDE network](#)
- [Wireless network security](#)
- [Protecting stored cardholder data](#)
- [Protecting communicated cardholder data](#)
- [Protecting the CDE network from viruses](#)
- [Monitoring the network for vulnerabilities](#)
- [Restricting access to cardholder data](#)
- [Controlling access to the CDE network](#)

Introduction to PCI DSS

The primary source of information for your PCI DSS compliance program is the Payment Card Industry (PCI) Data Security Standard itself. [Version 3.0](#) of the standard was published in November 2013. The following is only a brief summary of PCI DSS.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) sets data handling requirements for organizations that hold, process, or exchange cardholder information.

What is the Cardholder Data Environment

Throughout the PCI DSS requirements, there are references to the Cardholder Data Environment (CDE). The CDE is the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.

PCI DSS objectives and requirements

PCI DSS consists of 7 control objectives and 12 requirements.

PCI DSS Control Objectives and Requirements

Control Objective	Requirement	Fortinet Solution
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	FortiGate firewall functionality. See Security policies for the CDE network .
	2. Do not use vendor - supplied defaults for system passwords and other security parameters	FortiDB vulnerability assessment and auditing FortiWeb web application password checking See Password complexity and change requirements .
Protect Cardholder Data	3. Protect stored cardholder data	FortiDB vulnerability assessment and monitoring FortiWeb web application firewall See Protecting stored cardholder data .
	4. Encrypt transmission of cardholder data across open, public networks	FortiGate IPsec VPN. See Protecting communicated cardholder data .
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs	FortiGate integrated AV FortiClient integrated AV FortiMobile integrated AV FortiMail integrated AV FortiGuard automated AV updates See Protecting the CDE network from viruses .
	6. Develop and maintain secure systems and applications	FortiDB vulnerability assessment, auditing and monitoring FortiWeb web application security See Monitoring the network for vulnerabilities .

Control Objective	Requirement	Fortinet Solution
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know	FortiDB vulnerability assessment, auditing and monitoring. See Restricting access to cardholder data .
	8. Identify and authenticate access to system components	FortiGate integrated database or hooks to Active Directory. See Controlling access to the CDE network .
	9. Restrict physical access to cardholder data	Fortinet professional services in partnership with partner solutions
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	FortiDB auditing and monitoring FortiAnalyzer event reporting See Monitoring the network for vulnerabilities .
	11. Regularly test security systems and processes	FortiDB vulnerability assessment See Monitoring the network for vulnerabilities .
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	FortiManager security policy management appliance

This chapter describes how the FortiGate unit's features can help your organization to be compliant with PCI DSS. Requirements that the FortiGate cannot enforce need to be met through organization policies with some means determined for auditing compliance.

Be sure to read the section, [Wireless guidelines](#), below. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

Wireless guidelines

While wired networks usually connect fixed known workstations, wireless networks are more dynamic, introducing a different set of security concerns.

Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that unauthorized wireless networking has not been introduced into the CDE. Wireless networking could be introduced quite casually by adding a wireless device to a PC on the CDE network.

For all PCI DSS networks, whether they use wireless technology or not, the following requirement applies:

- Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. (11.1)

If your organization uses wireless networking outside the CDE network and the firewall prevents communication with the CDE network, the wireless network is outside the PCI DSS scope, but the firewall configuration must meet PCI DSS requirements.

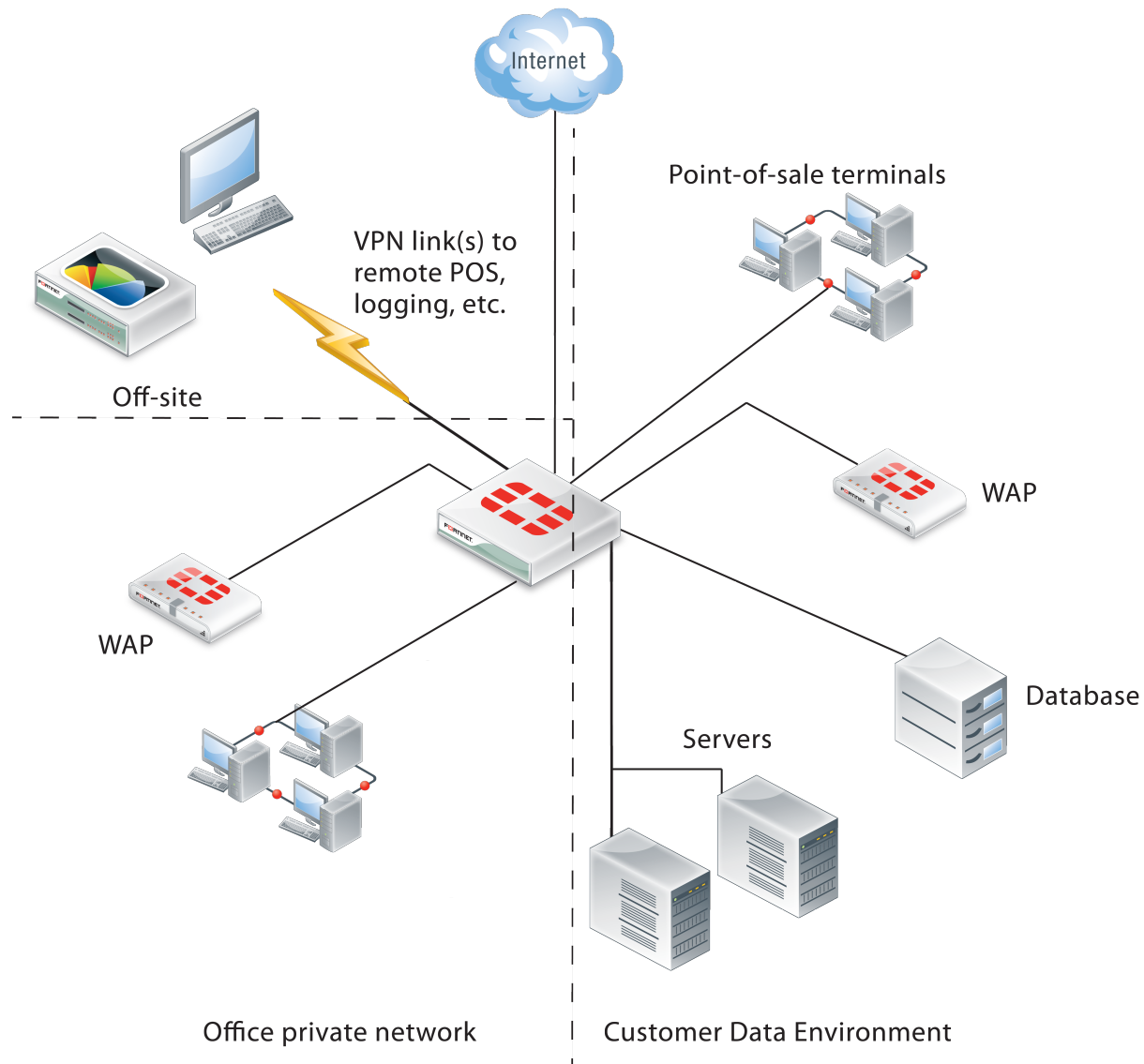
If your organization uses wireless networking inside the CDE network, the wireless network is within the PCI DSS scope. For information about wireless network requirements, see [Wireless network security](#).

Network topology

The cardholder data environment must be protected against unauthorized access from the Internet and from other networks in your organization. FortiGate unit firewall functionality provides tight control over the traffic that can pass between the following network interfaces:

- Internet
- CDE wired LAN
- CDE wireless LAN
- Other internal networks

The figure below shows how the Cardholder Data Environment can be delineated in a typical network.

Enterprise network with a cardholder data environment**Internet**

The FortiGate unit has at least one network interface connected to the Internet. If your organization uses more than one Internet service provider, there could be additional network interfaces that function as a route to the Internet.

The CDE wired LAN

The CDE network typically contains point-of-sale (POS) terminals, databases, and servers. The only security policies between the CDE network and the Internet should be for encrypted connections. For remote point-of-sale terminals or off-site databases, VPN connections are required and they should use strong encryption. For a web server that handles online purchases, only HTTPS (SSL or TLS) connections can be permitted. The security

policies that enable these connections should have the narrowest possible definitions for source address, destination address and service.

PCI DSS does not require the CDE network to be isolated from the rest of your corporate LAN. But isolating the CDE network reduces the scope of required data protection measures and may reduce the scope of PCI DSS assessments that are periodically required.

The CDE wireless LAN

Wireless networking is a special issue. Even if you do not use wireless technology you must monitor to ensure that unauthorized wireless access has not been added to the CDE network. For this purpose, the figure above shows a FortiAP device in the CDE. The FortiAP device can provide dedicated wireless monitoring, an access point, or both.

A small retail outlet could reduce costs by using a FortiWiFi unit, a FortiGate unit with integrated wireless networking. The FortiWiFi unit would have to be located where it could provide sufficient wireless monitoring (or access point) coverage for the entire premises.

Other internal networks

Other internal networks such as your office LAN, unless they provide connection to the CDE, are not subject to PCI DSS requirements.

Security policies for the CDE network

The FortiGate unit's firewall functionality is ideally suited to PCI DSS requirement 1.2.1, "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." Security policies control the source, destination, and type of traffic passing between networks.

The PCI DSS standard includes requirements to document your network topology and configuration. As part of that requirement, and to assist the auditing of your network, make use of the **Comment** field available in FortiGate security policies. Describe the purpose of each policy.

Controlling the source and destination of traffic

The source and destination are the first parameters you specify in a security policy. (Go to **Policy & Objects > Policy > IPv4** and select **Create New**.)

Incoming Interface	<input type="text" value="Click to add..."/>
Source Address	<input type="text" value="Click to add..."/>
Source User(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="Click to add..."/>
Outgoing Interface	<input type="text" value="Click to add..."/>
Destination Address	<input type="text" value="Click to add..."/>

The **Interface** settings depend on network topology. The **Address** settings define the IP addresses to which the policy applies. These should be as narrow as possible, so that only the appropriate hosts are included. For example, if the destination is a server with a single IP address, the named Destination Address should be defined as that single address, not the entire subnet on which the server resides.

Addresses are defined in **Policy & Objects > Objects > Addresses**. You can also define a new address by selecting **Create** from either the **Source Address** or **Destination Address** drop-down lists in a security policy. Some addresses will be used in several security policies, so it is best to plan ahead and define the addresses first.

Controlling the types of traffic in the CDE

The **Service** setting in each security policy determines which types of traffic can pass based on protocol.

You can select a single protocol from the **Service** drop-down list. To add another protocol, select the green “+” button to access the **Service** drop-down list again. If several security policies will need the same list of services, consider creating a named service group. (Go to **Firewall Objects > Service > Groups**.) In the security policy, service groups are available at the bottom of the **Service** drop-down list.

The default deny policy

All traffic not specifically allowed by a security policy that you create is blocked by the Implicit policy listed at the bottom of the **Policy & Objects > Policy > IPv4** page.

▼ Implicit (1)						
<input type="checkbox"/>	all	all	always	ANY	DENY	Implicit

You cannot delete this policy and you can edit the policy only to enable or disable logging of the traffic that it handles.

Wireless network security

Scanning for rogue access points is the minimum requirement for wireless security. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

If you use wireless networking, the wireless network is only within the PCI DSS scope if it can connect to the CDE.

On-wire detection of rogue APs

FortiGate units include an “on-wire” detection technique that correlates the SSID MAC addresses of the unknown access points with MAC addresses detected on your wired networks. This helps to differentiate unrelated neighboring APs from security-compromising unauthorized APs connected to your network.

Setting up rogue access point scanning

A FortiGate unit with a connected FortiAP unit can perform wireless scanning. Each of the FortiAP radios can act as a dedicated monitor or can perform scanning in the background while acting as a wireless access point.

Radio 1 operates in the 2.4GHz band and Radio 2 operates in the 5GHz band. Both bands should be monitored. The FortiAP unit(s) used for scanning must be located within the coverage area that would result if an access point were added to the CDE.

To configure rogue AP scanning in a FortiAP profile

1. Go to **WiFi Controller > WiFi Network > WIDS Profiles**.
On some models, the menu is **WiFi & Switch Controller**.
2. Select an existing WIDS profile and edit it, or select **Create New**.
3. Make sure that **Enable Rogue AP Detection** is selected.
4. Select **Enable On-Wire Rogue AP Detection**.
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Select **OK**.

Viewing the results of rogue AP scanning

Go to **WiFi Controller > Monitor > Rogue AP Monitor** to view information about detected wireless access points.

Logging the results of rogue AP scanning

To ensure that detection of rogue access points is logged, go to **Log & Report > Log Config > Log Settings** and enable logging for **WiFi activity event**.

Securing a CDE network wireless access point

If your wireless network is within PCI DSS scope, it must meet the following requirements:

- Default settings such as SSID and passphrases must be changed.
- Use WPA/WPA2 security.
- Log wireless activity.

Setting wireless security

On FortiGate units, go to **WiFi Controller > WiFi Network > SSID** to configure wireless security settings for either a new or existing virtual access point.

WiFi Settings

SSID	<input type="text" value="exampleSSID"/>
Security Mode	<input type="text" value="WPA2 Enterprise"/>
Authentication	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server
	<input type="text" value="Click to add..."/>

The default SSID for the FortiAP is “fortinet”. You must change this.

The **Security Mode** must be set to one of the WPA/WPA2 modes. Both WPA or WPA2 clients can be served. In the CLI, you can optionally select exclusively WPA or WPA2 operation.

WPA/WPA2-Enterprise **Authentication** uses separate logon credentials for each user. Either FortiGate user group security or an external RADIUS server performs the authentication. Optionally, certificate-based security can also be applied. WPA/WPA2-Personal authentication requires a single pre-shared key that is used by all clients and is thus less secure.

For detailed information about wireless access points, see the Deploying Wireless Networks chapter of the FortiOS Handbook.

Logging wireless network activity

To ensure that wireless network activity is logged, go to **Log&Report > Log Config > Log Settings** and enable logging for **WiFi activity event**.

Protecting stored cardholder data

The Fortinet FortiDB and FortiWeb products can provide security for your sensitive cardholder data.

The Fortinet Database Security (FortiDB) device provides vulnerability assessment, database activity monitoring, auditing and monitoring. For more information about this product, see the Fortinet website, www.fortinet.com.

The Fortinet FortiWeb Web Application Firewall deployed in front of public-facing web applications protects Web applications, databases, and the information exchanged between them. In particular, it addresses the PCI DSS requirements 6.5 and 6.6 regarding web application vulnerabilities such as cross-site scripting, SQL injection, and information leakage. For more information about this product, see the Fortinet website, www.fortinet.com.

Protecting communicated cardholder data

If cardholder data must be communicated over an untrusted network, such as the Internet, use the FortiGate unit's IPsec VPN capability to exchange the data securely. If you support customer online transactions, use HTTPS (SSL or TLS encryption) for security. The relevant PCI DSS requirement is:

- Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. (4.1)

This does not prescribe particular cryptography, but it can be interpreted as a requirement to follow industry best practices.

Configuring IPsec VPN security

The security considerations for IPsec VPNs are encryption and authentication.

Encryption

Go to **VPN > IPsec > Tunnels** to configure an IPsec VPN. In both Phase 1 and Phase 2 parts of the configuration, you select the encryption to use.

Encryption	3DES ▼	Authentication	SHA256 ▼
Encryption	AES128 ▼	Authentication	SHA256 ▼

These are advanced settings, overriding defaults that are not necessarily the strongest algorithms. VPNs negotiate over standards, so you can list multiple proposed algorithms. The VPN will use the strongest encryption that both ends support.

Choose strong encryption. The available encryption algorithms in descending order of strength are AES256, AES192, AES128, 3DES, DES. DES encryption is the weakest with only a 64-bit key and does not meet the 80-bit key length minimum that PCI DSS requires.

The message digest (authentication) algorithms in descending order of strength are SHA512, SHA384, SHA256, SHA1 and MD5. MD5 is particularly weak and should be avoided.

Authentication

VPN peers authenticate each other before establishing a tunnel. FortiGate units support two different authentication methods: pre-shared key and RSA signature (certificate). Certificates provide the best security. PCI DSS does not prohibit pre-shared keys, but you should limit access to the keys to the personnel who are responsible for the FortiGate units or other equipment at either end of the VPN.

Configuring SSL VPN security

The SSL VPN configuration includes a choice of encryption algorithm. You can only configure encryption key algorithms for SSL VPN in the CLI:

```
config vpn ssl settings
  set algorithm <low/medium/high>
end
```

The default option of **Medium** at **RC4 (128 bits)** is acceptable, but the **High** option, **AES (128/256 bits)** and **3DES** is more secure. The **Low** option, **RC4 (64 bits)**, **DES** and **higher** does not meet PCI DSS requirements.

Protecting the CDE network from viruses

PCI DSS requires the use of regularly updated antivirus protection. The antivirus functionality of the FortiGate unit protects both the FortiGate unit and the networks it manages. Workstations on these networks can be protected using FortiClient Endpoint Security. Both FortiGate and FortiClient antivirus protection can receive updates from Fortinet's FortiGuard service. Workstations can also use third-party antivirus applications with update services.

The FortiGate unit can enforce the use of antivirus software, denying unprotected workstations access to the network.

Enabling FortiGate antivirus protection

The antivirus profile must apply AV scanning to all protocols. You also need to enable SSL inspection to include secure protocols in antivirus scanning. The extended AV database contains the largest number of virus signatures.

To edit the antivirus profile

1. Go to **Security Profiles > AntiVirus**.
2. Edit the predefined profile or select **Create New**.

3. Set **Inspection Mode** to **Proxy**.
4. Ensure that all **Virus Scan** and **Block** check boxes are selected.
5. Select **Apply**.

To enable SSL inspection

1. Go to **Policy & Objects > Policy > SSL/SSH Inspection**.
On some models, the option is **SSL Inspection**.
2. Set **Inspection Method** to **Full SSL Inspection**.
3. Set each listed protocol to **On** and then select **Apply**.

To select the extended antivirus database

The antivirus database is selectable using the CLI:

```
config antivirus settings
    set default-db extended
end
```

For detailed information about the Antivirus feature, see the Security Profiles chapter of the FortiOS Handbook.

Configuring antivirus updates

On the system dashboard, check the **License Information** widget. The **Support Contract** section should show Valid Contract and the contract expiry date. If your FortiGate unit is not registered, you need to visit the Fortinet Support web page (<http://support.fortinet.com/>) to register. Go to Product Registration and follow the instructions.

In the **FortiGuard Services** section, check the **Antivirus** field. If the service is unreachable, see the online Help for information about troubleshooting your connectivity to FortiGuard Services.

Enforcing firewall use on endpoint PCs

PCI DSS requires you to “install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. (1.4)” Consider using the Endpoint Control feature of the FortiGate unit to enforce use of this software.

Monitoring the network for vulnerabilities

There are several tools that can assist you in monitoring your network for vulnerabilities and provide evidence to the PCI DSS auditor of such monitoring.

FortiGate logs

FortiGate units can be configured to send logs to FortiAnalyzer unit. In a larger network, this enables you to collect log information in a central location from several FortiGate units.

Using the FortiOS Network Vulnerability Scan feature

As part of its security features, FortiGate units provide a Network Vulnerability Scan. You define assets to monitor, such as servers, workstations, or point-of-sale terminals. Then, the FortiGate unit scans those devices on a regular schedule. The scan checks TCP and UDP ports against a list of known vulnerabilities provided by FortiGuard Services. Scan settings determine how many of the ports are checked. Optionally, all ports are scanned.

Vulnerability scanning options in the web-based manager are now hidden by default. To enable vulnerability scanning, go to **System > Config > Features**, select **Show More**, turn on **Vulnerability Scan**, and select **Apply**.

To set up vulnerability scanning, go to **User & Device > Vulnerability Scan > Scan Definition**. To view scan logs, go to **User & Device > Vulnerability Scan > Vulnerability Result**. For more information, see [Vulnerability Scan](#) in the Managing Devices chapter of the FortiOS Handbook.

Monitoring with other Fortinet products

In addition to your FortiGate unit and its FortiOS firmware, there are several other Fortinet products that can assist your organization to comply with PCI DSS requirements.

Fortinet Database Security (FortiDB)

A FortiDB appliance or FortiDB software can provide vulnerability scanning and activity monitoring for your databases. For more information about this product, see the Fortinet website, www.fortinet.com.

FortiWeb Web Application Security

If your organization engages in e-Commerce, you can use FortiWeb Application Security to protect your web servers against attack. The FortiWeb application protects against HTTP and XML-based attacks, guards against attempts to deface your websites, and scans web servers for vulnerabilities. For more information about this product, see the Fortinet website, www.fortinet.com.

Restricting access to cardholder data

In addition to security policies and authentication governing access to the CDE, you can deploy the Fortinet Database Security (FortiDB) device, which provides vulnerability assessment, database activity monitoring, auditing and monitoring. For more information about this product, see the Fortinet website, www.fortinet.com.

Controlling access to the CDE network

PCI DSS requires each user to be uniquely identified and authenticated. On the FortiGate unit, this applies to administrators and to users of SSL VPN and IPsec VPNs.

Password complexity and change requirements

By default, the FortiGate unit admin account has no password. Be sure to define a password.

PCI DSS password requirements are:

- Require a minimum length of at least seven characters. (8.2.3)
- Contain both numeric and alphabetic characters. (8.2.3)
- Change user passwords/passphrases at least every 90 days. (8.2.4)

To facilitate creation of compliant administrator passwords, you can set a password policy. Go to **System > Admin > Settings**. In the **Password Policy** section, enter the following and then select **Apply** at the bottom of the page.

☒ **Enable Password Policy**

Minimum Length (8-128 characters)

Must Contain at Least ☒

Upper Case Letters Lower Case Letters

Numbers (0-9) Special Characters

Apply Password Policy to ☒ Administrator Password ☐ IPsec Pre-shared Key

Enable Password Expiration ☒ (days)

Enable	Select the check box.
Minimum Length	8 or more. (Field does not accept a value less than 8.)
Must Contain	At minimum, set a required number of Numerical Digits and either Upper Case Letters or Lower Case Letters . Also setting a required number of Non-alphabetic Letters is acceptable.
Apply Password Policy to	Select Administrator Password .
Enable Password Expiration	Set to 90 days or less. The default is 90 days.

Note that the FortiGate password policy does not apply to user passwords. Both password complexity and password expiry for users would need to be addressed by making them a policy in your organization.

Password non-reuse requirement

PCI DSS requires that passwords are not re-used to satisfy the change requirement:

- Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. (8.2.5)

FortiGate users don't set their own passwords. The super_admin administrators can and so can admins with appropriate access. There is, however, no FortiGate-based mechanism to enforce non re-use of passwords.

Administrator lockout requirement

PCI DSS requires a user account lockout for administrators to guard against unauthorized access attempts:

- Limit repeated access attempts by locking out the user ID after not more than six attempts. (8.1.6),
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.1.7)

You can meet these requirements with the following CLI commands:

```
config system global
    set admin-lockout-threshold 6
    set admin-lockout-duration 1800
end
```

The threshold can be less than 6 and the lockout duration can be more than 1800.

Administrator timeout requirement

PCI DSS requires:

- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (8.1.8)

By default, the idle timeout is five minutes. You can go to **System > Admin > Settings** and change the **Idle Timeout** timeout to any value up to the permitted value of 15 minutes.

Administrator access security

To accommodate the requirement for unique identification of each user, the generic admin account should either be assigned to only one administrator or not used at all. You can create an administrator account for each administrator in **System > Admin > Administrators**.

If an administrator always works from the same workstation, consider using the Trusted Host feature. The administrator will be able to log in only from a trusted IP address. You can define up to three trusted IP addresses per administrator.

Administrative access must also be enabled per network interface. Go to **System > Network > Interface** to edit the interface settings. Enable administrative access only on interfaces where you would expect the administrator to connect. Allow only secure connection protocols, HTTPS for web-based access, SSH for CLI access.

Remote access security

For remote access, PCI DSS requires two-factor authentication: a password and some other authentication, such as a smart token or certificate. This applies to employees, administrators, and third parties.

SSL VPN users

For SSL VPN users, implement two-factor authentication by requiring users to have a certificate in addition to the correct password. Go to **VPN > SSL > Settings**, enable **Require Client Certificate**, and then select **Apply**. For more information, see the SSL VPN chapter of the FortiOS Handbook.

IPsec VPN users

If users access your network using an IPsec VPN, you can implement two-factor authentication by enabling extended authentication (XAUTH). This requires the user to enter a password in addition to the VPN authentication provided by the certificate or pre-shared key. As PCI DSS requires each user to have a unique identifier, you should already have user accounts and user groups defined.

To configure XAUTH on your VPN

1. Go to **VPN > IPsec > Tunnels** and create the new custom tunnel or edit an existing tunnel.
2. Edit the **Phase 1 Proposal** (if it is not available, you may need to click the Convert to Custom Tunnel button).
3. Under **XAuth**, select the **Server Type** setting, which determines the type of encryption method to use between the XAuth client, the FortiGate unit and the authentication server. Select one of the following options:
 - **PAP Server** —Password Authentication Protocol.
 - **CHAP Server** — Challenge-Handshake Authentication Protocol.
 - **Auto Server** —Use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server. This option allows multiple source interfaces to be defined in an IPsec/IKE policy.
4. From the **User Group** list, select the user group that needs to access the private network behind the FortiGate unit. The group must be added to the FortiGate configuration before it can be selected here. For multiple source interfaces to be defined in the IPsec/IKE policy, select **Inherit Groups from Policy**.
5. Select **OK**.



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.